CLAIMS

1. A method for authentication of a user by an authenticating entity comprising the steps of:

the authenticating entity sending a challenge to the user;

the user adding a spoiler to the challenge;

the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;

the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.

2. A method as claimed in claim 1, wherein the method includes the authenticating entity decrypting the encrypted combined spoiler and challenge using the public key of the asymmetric key pair and determining if the user has been authenticated.

3. A method as claimed in claim 1, wherein the addition of a spoiler to the challenge is carried out by applying a spoiler function to the challenge.

4. A method as claimed in claim 3, wherein the form of the spoiler function is sent to the authenticating entity.

5. A method as claimed in claim 1, wherein the spoiler is added to the challenge as a prefix or a suffix and the authenticating entity extracts the challenge by counting

the number of bytes from the beginning or end of the combined spoiler and challenge.

6. A method as claimed in claim 1, wherein the method includes the user obtaining a digest of the combined spoiler and challenge before the step of encrypting.

7. A method as claimed in claim 6, wherein the user obtains the digest by applying a hash function to the combined spoiler and challenge.

8. A method as claimed in claim 6, wherein the user sends details of the spoiler and the method of obtaining the digest to the authenticating entity.

9. A method as claimed in claim 1, wherein the user sends details of the algorithm used for encryption to the authenticating entity.

10. A method as claimed in claim 8, wherein the authenticating entity obtains a digest of the combined spoiler and the original challenge that the authenticating entity sent to the user and compares the digest to a digest obtained by decrypting the response from the user.

11. A method as claimed in claim 1, wherein the challenge is a bit sequence.

12. A method as claimed in claim 1, wherein the spoiler is an additional bit sequence.

13. A system for authentication of a user comprising a first application and an authenticating second application,

the authenticating second application having means for sending a challenge to the first application,

the first application having means for adding a spoiler to the challenge and means for encrypting the combined spoiler and challenge with a private key of an asymmetric key pair, and

means for sending the encrypted combined spoiler and challenge from the first application to the authenticating second application.

14. A computer program product stored on a computer readable storage medium for authentication of a user by an authenticating entity, comprising computer readable program code means for performing the steps of:

the authenticating entity sending a challenge to the user;

the user adding a spoiler to the challenge;

the user encrypting the combined spoiler and challenge using a private key of an asymmetric key pair;

the user sending a response to the authenticating entity in the form of the encrypted combined spoiler and challenge.